(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 869 863 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
09.08.2017 Bulletin 2017/32

(21) Application number: **06748565.6**

(22) Date of filing: **21.03.2006**

(51) Int Cl.:
H04L 29/06 *(2006.01)*

(86) International application number:
PCT/US2006/010460

(87) International publication number:
WO 2006/113036 (26.10.2006 Gazette 2006/43)

(54) **SECURED NETWORK PROCESSOR**

GESICHERTER NETZWERKPROZESSOR

PROCESSEUR DE RESEAU SECURISE

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

(30) Priority: **13.04.2005 US 105126**

(43) Date of publication of application:
26.12.2007 Bulletin 2007/52

(73) Proprietor: **The Boeing Company**
Chicago, IL 60606-1596 (US)

(72) Inventor: **PHAM, Tuan, A.**
Huntington Beach, California 92648 (US)

(74) Representative: **Howson, Richard G.B. et al**
Kilburn & Strode LLP
20 Red Lion Street
London WC1R 4PJ (GB)

(56) References cited:
WO-A-03/021866 WO-A2-01/26338

- **AECC: "Draft 3 of ARINC project paper 664:Aircraft data network, Part 5: Network domain characteristics and interconnection" AEEC, [Online] 4 November 2004 (2004-11-04), XP002398177 Retrieved from the Internet: URL:http://web.archive.org/web/20050205154616/www.arinc.com/aeec/draft_documents/664p5_d3.pdf>**
- **AECC: "Draft 4 of supplement 1 to ARINC Specification 664:Aircraft data network, Part 4: Internet-based Address Structure & Assigned numbers" AECC, [Online] 4 November 2004 (2004-11-04), XP002398178 Retrieved from the Internet: URL:http://web.archive.org/web/20050205160353/www.arinc.com/aeec/draft_documents/664p4_d4s1.pdf>**
- **USAF Airborne Network Special Interest Group: "AIRBORNE NETWORK ARCHITECTURE", , 7 October 2004 (2004-10-07), Retrieved from the Internet: URL:http://folk.uio.no/paalee/referencing_publications/ref-nr-airborne-report04.doc [retrieved on 2012-03-26]**

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 1 869 863 B1

Description

BACKGROUND OF THE INVENTION

Field Of the Invention

[0001] The present invention relates to a system and method for network communication, and more particularly, to a system and method for processing legacy radio signals.

Background

[0002] Aircrafts (or other transport systems) are monitored by a central network computing system located at a network operation center ("NOC"). It is desirable for the NOC to have a global view of various aircrafts (military and/or commercial), whether grounded or in air. Hence, it is important for transport systems (e.g. aircrafts) to efficiently receive and process plural data inputs.

[0003] In the past, multiple single-band radio systems have been used for communication between transport units and NOCs. Such radio systems (referred to as "legacy radio" systems), are often incompatible with each other and with modern radio systems.

[0004] The U.S. Department of Defense has created radio system designs, such as the Joint Tactical Radio System (JTRS) to provide Internet Protocol (IP) radio interfaces for modern and legacy platforms. However, these systems require expensive retrofit programs and development of new avionics software.

[0005] Conventional systems process inputs from plural radio links using custom software/hardware interfaces. Every time a new link is added to an aircraft, new application specific hardware/software is needed to process data inputs.

[0006] Conventional military systems do not have enabling web (or Internet) service software technologies to facilitate data sharing between incompatible networks. Without standard software interfaces, a legacy radio digital link would require extensive application/platform specific software so that information can be exchanged between one platform/network to another (i.e. for machine-to-machine interface). The lack of this machine-to-machine interface for legacy systems has largely prohibited these dissimilar systems/networks from rapidly sharing information among themselves and others.

[0007] Conventional systems do not provide an integrated solution that can efficiently process data inputs from legacy radio links. Also, especially in aviation systems, securing communication is very important. Conventional systems are not able to categorize data inputs based on their security level and process them accordingly.

[0008] Therefore, what is desired is a method and system that can efficiently process data inputs from legacy radio links and/or other input sources.

[0009] WO 03/021866 relates to a communications system that provides broadband access to passengers of mobile platforms includes a router located on the mobile platform.

[0010] http://web.archive.org/web/20050205154616/www.arinc.com/aeec.draf t documents/664p5_d3.pdf relates to an aircraft data network, network domain characteristics and interconnection.

[0011] http://folk.uio.no/paalee/referencing publications/ref-nr-airborne-report04.doc relates to airborne network architecture.

[0012] WO 01/26338 relates to vehicle internetworks provide for communications among diverse electronic devices within a vehicle, and for communications among these devices and networks external to the vehicle.

[0013] The present invention is set out in the independent claims, with some optional features set out in the claims dependent thereto.

SUMMARY OF THE INVENTION

[0014] In one aspect of the present invention, a system for sharing data between networks comprises an interface for receiving data from plural inputs; a policy-based router receiving data from plural inputs; a policy-based router operationally connected to the interface, the policy-based router assigns security levels to the data based on security characteristics of the inputs and assigns virtual Internet protocol addresses to the data; a translator for converting the data into a standard format; and a network stack for transmitting the data to a network.

[0015] In another aspect of the present invention, a method for sharing data between networks comprises receiving data from plural inputs; assigning security levels to the data based on security characteristics of the inputs; assigning virtual Internet protocol addresses to the data; retaining the data with the Internet protocol addresses; converting the data into a standard format; and transmitting the data to a network.

[0016] This brief summary has been provided so that the nature of the invention may be understood quickly. A more complete understanding of the invention can be obtained by reference to the following detailed description of the preferred embodiments thereof in connection with the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] The foregoing features and other features of the present invention will now be described with reference to the drawings of a preferred embodiment. In the drawings, the same components have the same reference numerals. The illustrated embodiment is intended to illustrate, but not to limit the invention. The drawings include the following Figures:

Figure 1 is a block diagram of a system for exchanging data between networks, according to an embod-

iment of the present invention;
Figure 2 is a block diagram showing the internal functional architecture of an on-board computing system shown in Figure 1;
Figure 3 is a block diagram of a system for secured communication between networks, according to another embodiment of the present invention;
Figure 4 is a block diagram of an exemplary secured network processor, according to another embodiment of the present invention;
Figure 5 is a flow chart of a method for communicating between networks, according to an embodiment of the present invention;
Figure 6 is a flow chart of another method for communicating between networks, according to a further embodiment of the present invention; and
Figure 7 is a flow chart of yet another method for communicating between networks, according to a still further embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0018] The following detailed description is of the best currently contemplated modes of carrying out the invention. The detailed description is not to be taken in a limiting sense, but the detailed description is made merely for the purpose of illustrating the general principles of the invention, since the scope of the invention is best defined by the appended claims.

[0019] To facilitate an understanding of the preferred embodiment, the general architecture and operation of an on-board computing system will be described. The specific architecture and operation of the preferred embodiments will then be described with reference to the general architecture.

Network Centric Operations (NCO) Architecture:

[0020] Figure 1 is a block diagram of a system 10 for communicating data between networks. An off-board communications domain may comprise a Beyond Line-Of-Sight Data Input Source 12 and a Line-Of-Sight Data Input Source 14.

[0021] The Beyond Line-Of-Sight Data Input Source 12 includes satellite-based sources, of over about 600 miles (about 966 kilometers) in range, such as ultra-high frequency and very high frequency satellite communications (UHF/VHF SATCOM), international marine and maritime satellite communications (INMARSAT), Aircraft Communications Addressing and Reporting System (ACARS), Family of Advanced Beyond-Line-of-Sight Terminals (FAB-T), and the like.

[0022] The Line-Of-Sight Data Input Source 14 includes sources, with about 0-30 miles (up to about 48.28 kilometers) in range, such as LINK-16 (a military intercomputer data exchange format), Flying Local Area Network (FLAN), Wideband Network Waveform of the Joint Tactical Radio System (JTRS WNW), and the like.

[0023] The Beyond Line-Of-Sight Data Input Source 12 and the Line-Of-Sight Data Input Source 14 communicate with an on-board computing system 16, which comprises of a secured network processor 18.

[0024] It is noteworthy that the present invention is not limited to a particular number of on-board computing systems 16. Any number of on-board computing systems 16 that can be connected to the Internet 20 or any other computer network may be used.

[0025] The on-board computing system 16 may be installed aboard a vehicle (not shown), such as a spacecraft, an aircraft, a tank, an automobile, a vessel, and the like. Although the following description uses an aircraft as an exemplary embodiment, it is to be understood that the present invention may be practiced with all types of vehicles or on foot. For example, the on-board computing system 16 may be installed aboard an automobile.

[0026] Furthermore, it is to be understood that the present invention may be practiced at stationary or movable locations. For example, the on-board computing system 16 may be installed aboard a moving vehicle as well as being installed at a fixed building, such as a ground-based air traffic control station.

[0027] The term "data" is to be understood in the description to include any type of information. For example, the data communicated or exchanged may be of any type of information, including one of the groups consisting of control data, audio, voice, image, and video.

[0028] The Beyond Line-Of-Sight Data Input Source 12, the Line-Of-Sight Data Input Source, and the on-board computing system 16 may exchange data with a network operation center 22 via any network, for example, the Internet 20.

Computer System Architecture

[0029] Figure 2 is a block diagram showing the internal functional architecture of the on-board computing system 16, exclusive of the secured network processor 18. The secured network processor 18 will be described below regarding Figure 3. As shown in Figure 2, system 16 includes a central processing unit (CPU) 26 for executing computer-executable process steps. CPU 26 interfaces with a computer bus 24. Also shown in Figure 2 is a secured network processor interface (I/F) 28, which may be operationally coupled to the secured network processor 18 (shown in Figure 1).

[0030] A random access main memory ("RAM") 30 may also be operationally coupled to interface with computer bus 24 to provide CPU 26 with access to memory storage when executing stored computer-executable process steps from storage 38. Storage 38 may comprise storage media such as a floppy disk, a hard disk, a compact disc (CD), a digital versatile disk (DVD), and the like. CPU 26 stores and executes the process steps out of RAM 30. Items operationally coupled to the computer bus 24 may be hardware-based or software-based.

[0031] Auxiliary interfaces 32 and 34 may be operationally coupled to the computer bus 24 to interface with other desired components, such as a navigational system (not shown), a global positioning satellite (GPS) system (not shown), a laser system (not shown), or a microwave signal system (not shown).

[0032] A network interface 36 may be operationally coupled to the computer bus 24 to interface with any of several networks (not shown).

[0033] Read only memory ("ROM") 40 may be operationally coupled to the computer bus 24 to store invariant instruction sequences such as start-up instruction sequences or basic input/output operating system (BIOS) sequences for the secured network processor 18 (shown in Figure 1).

[0034] Continuing with Figure 2, an audio interface 42 and a video interface 44 may be operationally coupled to the computer bus 24 for interfacing with audio equipment and video equipment, respectively.

[0035] The following provides a description of the Internet that can used for communication among various components of system 10 (Figure 1).

The Internet:

[0036] The Internet 20 connects thousands of computers world wide through well-known protocols, for example, Transmission Control Protocol (TCP)/Internet Protocol (IP), into a vast network. TCP/IP is a communications protocol developed under contract from the United States Department of Defense to internetwork dissimilar systems. TCP/IP is the de facto UNIX standard protocol of the Internet and the global standard for communications. Every client and server in a TCP/IP network requires an IP (Internet Protocol) address, which is either permanently assigned or dynamically assigned at startup.

[0037] Information on the Internet 20 is stored world wide as computer files, mostly written in the Hypertext Mark Up Language ("HTML"). Other mark up languages, e.g., Extensible Markup Language ("XML") as published by W3C Consortium, Version 1, Second Edition, October 2000, ©W3C may also be used.

[0038] The collection of all such publicly available computer files is known as the World Wide Web ("WWW"). The WWW is a multimedia-enabled hypertext system used for navigating the Internet 20 and is made up of hundreds of thousands of web pages with images and text and video files, which can be displayed on a computer monitor. Each web page can have connections to other pages, which may be located on any computer connected to the Internet 20.

[0039] A typical Internet 20 user uses a client program called a "Web Browser" to connect to the Internet 20. The web browser may run on any computer connected to the Internet 20. Currently, various browsers are available of which two prominent browsers are Netscape Navigator and Microsoft Internet Explorer.

[0040] The Web Browser receives and sends requests to a web server and acquires information from the WWW. A web server is a program that, upon receipt of a request, sends the requested data to the requesting user. A standard naming convention known as Uniform Resource Locator ("URL") has been adopted to represent hypermedia links and links to network services. Most files or services can be represented with a URL.

[0041] URLs enable Web Browsers to go directly to any file held on any WWW server. Information from the WWW is accessed using well-known protocols, including the Hypertext Transport Protocol ("HTTP"), the Wide Area Information Service ("WAIS") and the File Transport Protocol ("FTP"), over TCP/IP protocol. The transfer format for standard WWW pages is Hypertext Transfer Protocol (HTTP).

COMMUNICATING BETWEEN SECURED NETWORK PROCESSORS:

[0042] Figure 3 shows a block diagram of a system 100 for communicating between networks. A plurality of application interfaces 102A-102D may be operationally coupled to a secured network processor (SNP) 104 (similar to SNP 18, Figure 1). A plurality of non-IP radio links 106A-106D may be used to exchange data between the secured network processor 104 and another secured network processor 108. Another plurality of application interfaces 110A-110D may be operationally coupled to the secured network processor 108.

[0043] The secured network processors 104, 108 may be installed at separate locations. For example, the secured network processor 104 may be situated at a ground station (not shown) while the secured network processor 108 may be situated aboard an aircraft (not shown). The ground station (not shown) and the aircraft (not shown) may communicate via the non-IP radio links 106A-106D.

[0044] In another embodiment, the secured network processor 104 may be situated aboard a first aircraft (not shown) and the secured network processor 108 may be situated aboard a second aircraft (not shown). The first aircraft (not shown) and the second aircraft (not shown) may communicate via the non-IP radio links 106A-106D.

[0045] In the secured network processor 104 a policy-based router 112 serves to direct the exchange of data between the application interfaces 102A-102D and a plurality of legacy non-IP radio links (or interfaces/devices) 114, 116, 118, and 120 (may also be referred to as modules 114, 116, 118 and 120). The policy-based router 112 may be a secured IP network router.

[0046] As data is communicated, via non-IP radio links (or non-IP radio connection) 106A-106D (may also be referred to as links 106A-106D), from the secured network processor 104 to the secured network processor 108, data may be received at a plurality of legacy non-IP radio links (interfaces) 122, 124, 126, 128 (may also be referred to as modules 122, 124, 126 and 128). A policy-based router 130 serves to direct the exchange of

data between modules 122, 124, 126, 128 and a plurality of application interfaces 110A-110D.

[0047] Figure 4 shows a block diagram of information flow through the secured network processor 108. It is to be understood that the flow of information in secured network processor 108 is exemplary and that a similar flow of information, in reverse, is correspondingly contemplated for secured network processor 104.

[0048] Data may be sent to the secured network processor 108 via any one or more of a plurality of links 106A-106D. Any one or more of the plurality of links 106A-106D may communicate with any one or more of a plurality of modules 122-128.

[0049] The data may be exchanged among any one or more of a plurality of modules 122-128, the policy-based router 130, and any one or more of a plurality of network stacks 170A-170D.

[0050] The network stacks 170A-D direct data in cooperation with the policy-based router 130, to any one or more of a plurality of application interfaces 110A-110D. From the application interfaces 110A-110D, the data is sent to one or more networks 208A-208D, respectively.

[0051] The policy-based router 130 determines the security level of the data arriving through the non-IP radio links 106A-106D, depending on the security characteristics of the data. Some data may be characterized as having a secret level (i.e. high security level, such that the data comprises classified information, such as military intelligence data. Some data may be characterized as having an unclassified-but-sensitive (UBS) level, such that the data does not comprise classified information but the data does comprise information to be kept confidential (such as passenger or crew identity). Some data may be characterized as not having a secret or a UBS level (i.e. unsecured). Lastly, some data may be characterized as having security levels in between the security levels described above.

MODULES 122-128:

[0052] Each of modules 122-128 comprises an interface, a data exchange format component, and a format translator, such as an XML translator (for example, the ECS/XML processor available from Electronic Commerce Solutions, Limited of Horsham in the United Kingdom).

[0053] For example, module 122 may comprise a terminal interface 172 (such as the Nais model available from the Matsushita Electrical Industrial Company, Limited of Osaka, Japan), a LINK-16 component 180 (providing an inter-computer data exchange format), a Variable Message Format (VMF) component 182, and an XML translator 192 for converting data into an XML format.

[0054] The terminal interface 172 may be a radio control interface (hardware and software) that keeps a link active (such as a USB bus or a 1553 bus). The terminal interface 172 can receive the data from link 106A, reformat the data, parse the data, recognize the data, and align the data.

[0055] VMF is a member of the J-Series family of message formats, along with Link-16, Link-22, and the Common Message Format (CMF). VMF messages provide a common means of exchanging data across any interface with varying needs for volume and detail of information, and applicable to a broad range of communications systems.

[0056] Continuing with Figure 4, module 124 may comprise a modem I/M (intermodulation) component 174, a LINK 11A component 184 (processing half-duplex, netted links), a LINK 11B component 186 (processing full duplex, point-to-point links), and an XML translator 194.

[0057] Module 126 may comprise an Ethernet converter 176 (such as the ORiNOCO Ethernet Converter RS232 available from the Proxim Corporation of Sunnyvale, California in the United States), a TCP/IP component 188, and an XML translator 196.

[0058] Module 128 may comprise a network interface card (NIC) 178 (such as the Linksys USB100TX Etherfast 10/100 USB Adapter available from Cisco Systems, Incorporated of Irvine, California in the United States), a TCP/IP component 190, and an XML translator 198.

[0059] XML translators 192, 194, 196 and 198 receive inputs from plural sources as shown in Figure 4. The XML translators convert data from a legacy format to a standard, platform independent format.

[0060] It is noteworthy that modules 122, 124, 126 and 128 are similar to modules 114, 116, 118 and 120 (Figure 3).

POLICY-BASED ROUTER:

[0061] The policy-based router 130 (or 112, Figure 3) may be operationally coupled to modules 122-128. The policy-based router 130 determines the ultimate destination of the data (such as networks 208A-208D) depending upon the security level of the data, sending the data through one of the network stacks 170A-170D, and through a corresponding application interface 110A-110D.

[0062] A security module 200 is used to choose which appropriate network stack 170A-170D to send the data based on the security level of the data. The security module 200 could be hardware-based or software-based. A processor 202 is used to execute instructions, via a software interface 206, regarding the path of data through the secured network processor 108.

[0063] The policy-based router may have a static IP address. The policy-based router assigns dynamic virtual IP addresses, with reference to a virtual IP address table 204, to the data, depending upon the appropriate security level.

[0064] For example, if network 208A is intended for secret level data, a virtual IP address would be assigned to the secret level data. The secret level data would then be sent through a network stack 170A, limited to secret

level data throughput, for transmittal to the secret level network 208A through the application interface 110A, which is also limited to secret level data throughput.

[0065] Likewise, if network 208B is intended for UBS level data, a virtual IP address would be assigned to the UBS level data. The UBS level data would be sent through a network stack 170B, limited to UBS level data throughput, for transmittal to the UBS level network 208B through the application interface 110B, which is also limited to UBS level data throughput.

[0066] Similarly, any non-secure data may be directed to non-secure networks (for example, network 208C or network 208D) through non-secure network stacks (for example, network stack 170C or network stack 170D), through application interfaces (for example, application interface 110C or application interface 110D) for transmittal to non-secure networks (for example, network 208C or network 208D). Virtual IP addresses would be assigned to the non-secure data.

NETWORKS:

[0067] The networks 208A-208D may be any type of network supporting flight systems on an aircraft. For example, network 208A may be an avionics domain network. Network 208B may be an on-board C2ISR (command, control, intelligence, surveillance, and reconnaissance) network. Network 208C may be a delivery domain network, pertaining, for example, to cargo tracking systems, such as Radio Frequency Identification (RFID) or pertaining to a Flight Control System (FCS) and network 208D may be a registry domain network.

METHOD OF FORWARD LINKING DATA BETWEEN NETWORKS:

[0068] Figure 5 shows a flow chart of a method 210 for forward linking data between networks (for example, data output from a secured network processor). In step S212, XML data is received by router 130. For example, application interface 110A sends XML data to router 130.

[0069] In step S214, router 130 determines if any type of encryption is required. This determination is based on the type of data and the destination. As discussed above, some links are secured to handle secured communication, while others are unsecured. In one aspect, an application interface (for example, 110A) sets a flag that notifies router 130 whether encryption is needed.

[0070] If encryption is needed, then in step S216, secure module 200 encrypts the data. Secure module 200 may use any type of security algorithm to encrypt the received data. For example, SSL (secured socket layer) or Advanced Encryption Standard (AES) may be used to encrypt the data. It is noteworthy that the adaptive aspects of the present invention are not limited to any particular type of encryption technique or system. If encryption is not needed, then the process moves to step S218.

[0071] In step S218, router 130 assigns a virtual IP address to the packet. This is based on a virtual IP address table 204.

It is noteworthy that an aircraft itself is assigned a unique IP address. Communication that is being sent from the aircraft via specific links is assigned virtual IP addresses.

[0072] In step S220, router 130 generates IP packets. In step S222, router 130 using security module 200 assigns a particular security level (for example, very secured, secured, UBS, or non-secured) for the IP packet. The level of security on a link and the assignment is based on the type of packet, i.e., a higher security level is assigned to a packet that requires higher security, whereas, a lower security level is assigned to a packet that requires lower security. This ensures that the packet is sent via a secured or unsecured link depending on the type of packet. Router 130 firmware may use a security setting table (not shown) to set the appropriate security level.

[0073] In step S224, router 130 assembles the frame and then in step S226, router 130 sends the frame to an output queue (not shown).

[0074] In step S228, the appropriate link is assigned for the packet. Router 130 may use standard rules to assign the appropriate link.

[0075] In step S230, the packet is placed in a queue for a specific link and in step S232, router 130 sends the packet via the assigned link. Router 130 continues to monitor the link to ensure that the packet has been sent. If the packet is successfully sent, then the process ends in step S236. If the link fails to send the packet, then the process reverts back to step SS228.

METHOD OF REVERSE LINKING DATA BETWEEN NETWORKS:

[0076] Figure 6 shows a flow chart of a method 250 for reverse linking data between networks (for example, data input to a secured network processor). In step S252, data is received at a terminal interface. For example, as shown in Figure 4, terminal interface 172 receives data via radio link 106A.

[0077] In step S254, router 130 confirms if a message has been received properly. If not, then SNP 108 waits for the message.

[0078] If a message is properly received, then in step S258, the message is translated into a standard format. For example, XML translator 192 translates the data received via terminal interface 172 into an XML format.

[0079] In step S260, the frame is assembled by module 192 for a frame queue (not shown). The frame queue is used by router 130 to assign priority for processing frames.

[0080] In step S262, router 130 determines if any encryption has been applied. This is based on the type of data that is received and/or the destination to which the frame will be sent by router 130. If encryption has been applied, then the packet is decrypted by security module 200. If encryption is not applied, then the process moves

to step S266.

[0081] In step S266, router 130 extracts the IP packets. In step S268, the packet is assigned a security level and priority level by router 130. The security level may be high, medium or low, based on packet content and/or packet destination.

[0082] In step S270, the packets are forwarded by router 130 and placed in an output queue. In step S272, the XML data is transmitted to the appropriate destination, via a network stack and application interface.

METHOD OF SHARING DATA BETWEEN NETWORKS:

[0083] Figure 7 shows a flow chart of a method 310 for sharing data between networks. The method 310 comprises a step S312 of receiving data from plural inputs. The plural inputs may be radio inputs. The data may be any type of information, such as information that includes one of the groups consisting of control data, audio, voice, image, and video.

[0084] In step S314, data received from the radio links is converted into a standard format, for example, the XML format (using XML translator 192).

[0085] In step S316, router 130 assigns security levels to the data based on security characteristics of the inputs and the destination of the packets. In step S316, router 130 assigns virtual Internet protocol addresses using virtual IP address table 204. In step S320, the data, in a standard format, is transmitted to the appropriate destination.

[0086] In one aspect of the present invention, an integrated system is provided, that receives inputs from plural disparate sources, converts the data into a standard format and based on the type of data and destination, the data is transmitted. This system is scalable, modular and efficient.

[0087] Although the present invention has been described with reference to specific embodiments, these embodiments are illustrative only and not limiting. Many other applications and embodiments of the present invention will be apparent in light of this disclosure and the following claims.

Claims

1. A system for sharing data between networks, comprising:

   an interface for receiving data from plural of non Internet protocol radio link inputs;
   a policy-based router operationally connected to the interface, wherein the policy-based router is adapted to assign security levels to the data based on security characteristics of the inputs and the policy-based router is adapted to assign dynamic virtual Internet protocol addresses to the data depending on the assigned security level;
   a memory for retaining the data with the Internet protocol addresses, the memory being operationally connected to the policy-based router;
   a translator for converting the data into a standard format; and
   a network stack for transmitting the converted data to a network.

2. The system of Claim 1, wherein the standard format includes an XML format.

3. The system of Claim 1, wherein the data includes control data, audio, voice, image, and video.

4. The system of Claim 1, wherein an on-board computing system is adapted to share data packets with another aircraft and/or a network operation center.

5. A method for sharing data between networks, comprising the steps carried out by a computing system of:

   receiving data from plural of non Internet protocol radio link inputs;
   assigning security levels to the data based on security characteristics of the inputs;
   assigning dynamic virtual Internet protocol addresses to the data depending on the assigned security level;
   retaining the data with the Internet protocol addresses;
   converting the data into a standard format; and
   transmitting the converted data to a network.

6. The method of claim 5, wherein the converting step includes converting the data into an XML format.

7. The method of claim 5, wherein the data includes control data, audio, voice, image, and video.

8. The method of Claim 5, wherein an on-board computing system shares data packets with an aircraft and/or a network operation center.

Patentansprüche

1. System zum Austausch von Daten zwischen Netzwerken, aufweisend:

   eine Schnittstelle zum Empfangen von Daten von mehreren Nicht-Internetprotokoll-Funkverbindungs-Eingängen;
   einen richtlinienbasierten Router, der wirkmäßig mit der Schnittstelle verbunden ist, wobei der richtlinienbasierte Router dafür geeignet ist, den

Daten basierend auf Sicherheitsmerkmalen der Eingänge Sicherheitsstufen zuzuweisen und wobei der richtlinienbasierte Router dafür geeignet ist, den Daten in Abhängigkeit von der zugewiesenen Sicherheitsstufe dynamische virtuelle Internetprotokolladressen zuzuweisen;
einen Speicher zum Speichern der Daten mit den Internetprotokolladressen, wobei der Speicher wirkmäßig mit dem richtlinienbasierten Router verbunden ist,
einen Übersetzer zum Konvertieren der Daten in ein Standardformat; und
einen Netzwerkstapel zum Senden der konvertierten Daten an ein Netzwerk.

2. System nach Anspruch 1, wobei das Standardformat ein XML-Format beinhaltet.

3. System nach Anspruch 1, wobei die Daten Steuerdaten, Audio-, Stimm-, Bild- und Videoinformationen beinhalten.

4. System nach Anspruch 1, wobei ein Bordrechensystem dafür geeignet ist, Datenpakete mit einem anderen Flugzeug und/oder einem Netzwerkbetriebszentrum auszutauschen.

5. Verfahren zum Austausch von Daten zwischen Netzwerken, aufweisend die folgenden, von einem Rechensystem ausgeführten Schritte:

Empfangen von Daten von mehreren Nicht-Internetprotokoll-Funkverbindungs-Eingängen;
Zuweisen von Sicherheitsstufen an die Daten basierend auf Sicherheitsmerkmalen der Eingänge;
Zuweisen von dynamischen virtuellen Internetprotokolladressen an die Daten in Abhängigkeit von der zugewiesenen Sicherheitsstufe;
Speichern der Daten mit den Internetprotokolladressen;
Konvertieren der Daten in ein Standardformat; und
Senden der konvertierten Daten an ein Netzwerk.

6. Verfahren nach Anspruch 5, wobei der Konvertierungsschritt das Konvertieren der Daten in ein XML-Format beinhaltet.

7. Verfahren nach Anspruch 5, wobei die Daten Steuerdaten, Audio-, Stimm-, Bild- und Videoinformationen beinhalten.

8. Verfahren nach Anspruch 5, wobei ein Bordrechensystem Datenpakete mit einem Flugzeug und/oder einem Netzwerkbetriebszentrum austauscht.

Revendications

1. Système de partage de données entre réseaux, comprenant :

une interface afin de recevoir des données à partir d'une pluralité d'entrées de liaison radio de protocole non Internet ;
un routeur basé sur un programme, connecté de manière opérationnelle à l'interface, dans lequel le routeur basé sur un programme est adapté pour attribuer des niveaux de sécurité aux données en fonction des caractéristiques de sécurité des entrées et le routeur basé sur un programme est adapté pour affecter des adresses dynamiques virtuelles de protocole Internet aux données en fonction du niveau de sécurité attribué ;
une mémoire pour conserver les données avec les adresses de protocole Internet, la mémoire étant opérationnellement connectée au routeur basé sur un programme ;
un traducteur afin de convertir les données en un format standard ; et
une pile de réseau afin de transmettre les données converties à un réseau.

2. Le système de la revendication 1, dans lequel le format standard comprend un format XML.

3. Le système de la revendication 1, dans lequel les données comprennent des données de contrôle, audio, vocales, images et vidéo.

4. Le système de la revendication 1, dans lequel un système informatique embarqué est adapté afin de partager des paquets de données avec un autre avion et / ou un centre d'opération de réseau.

5. Un procédé de partage de données entre réseaux, comprenant les étapes mises en oeuvre par un système informatique consistant à :

recevoir des données à partir d'une pluralité d'entrées de liaison radio de protocole non Internet ;
attribuer des niveaux de sécurité aux données en fonction des caractéristiques de sécurité des entrées ;
attribuer des adresses dynamiques virtuelles de protocole Internet aux données en fonction des caractéristiques de sécurité des entrées ;
conserver les données avec les adresses de protocole Internet ;
convertir les données en un format standard ; et
transmettre les données converties à un réseau.

6. Le procédé de la revendication 5, dans lequel l'étape

de conversion comprend la conversion des données en un format XML.

7. Le procédé de la revendication 5, dans lequel les données comprennent des données de contrôle, audio, vocales, images et vidéo.

8. Le procédé de la revendication 5, dans lequel un système informatique embarqué partage des paquets de données avec un autre avion et / ou un centre d'opération de réseau.

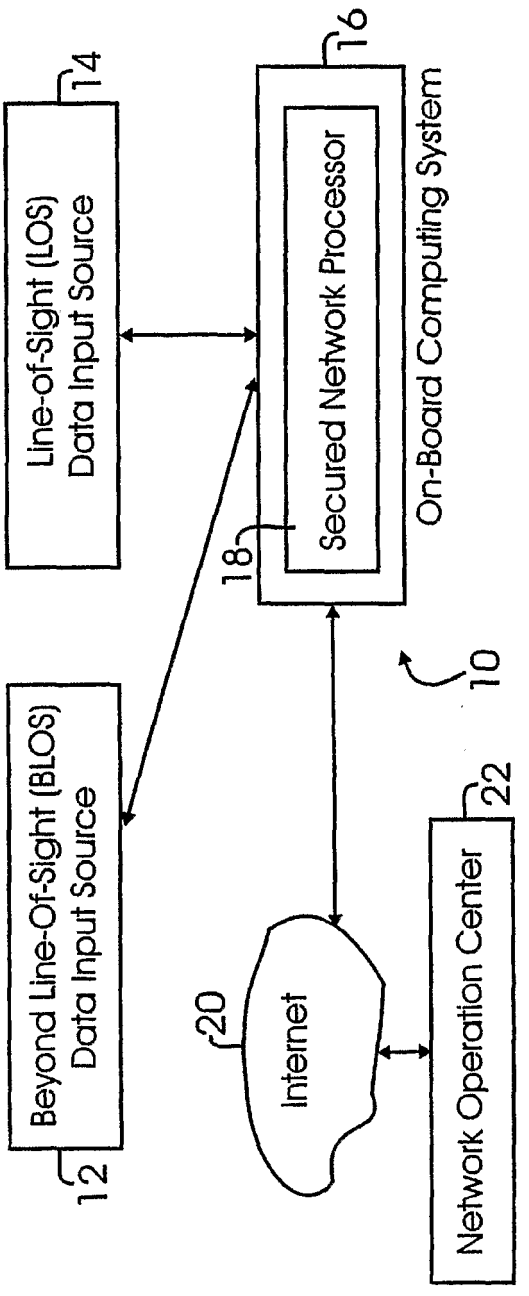


Figure 1

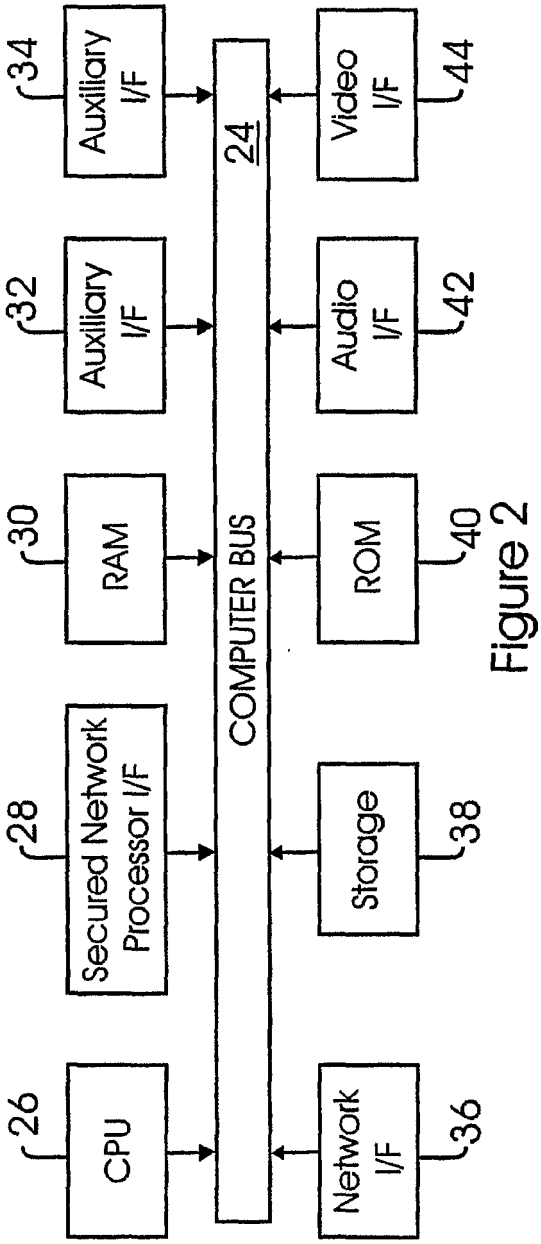


Figure 2

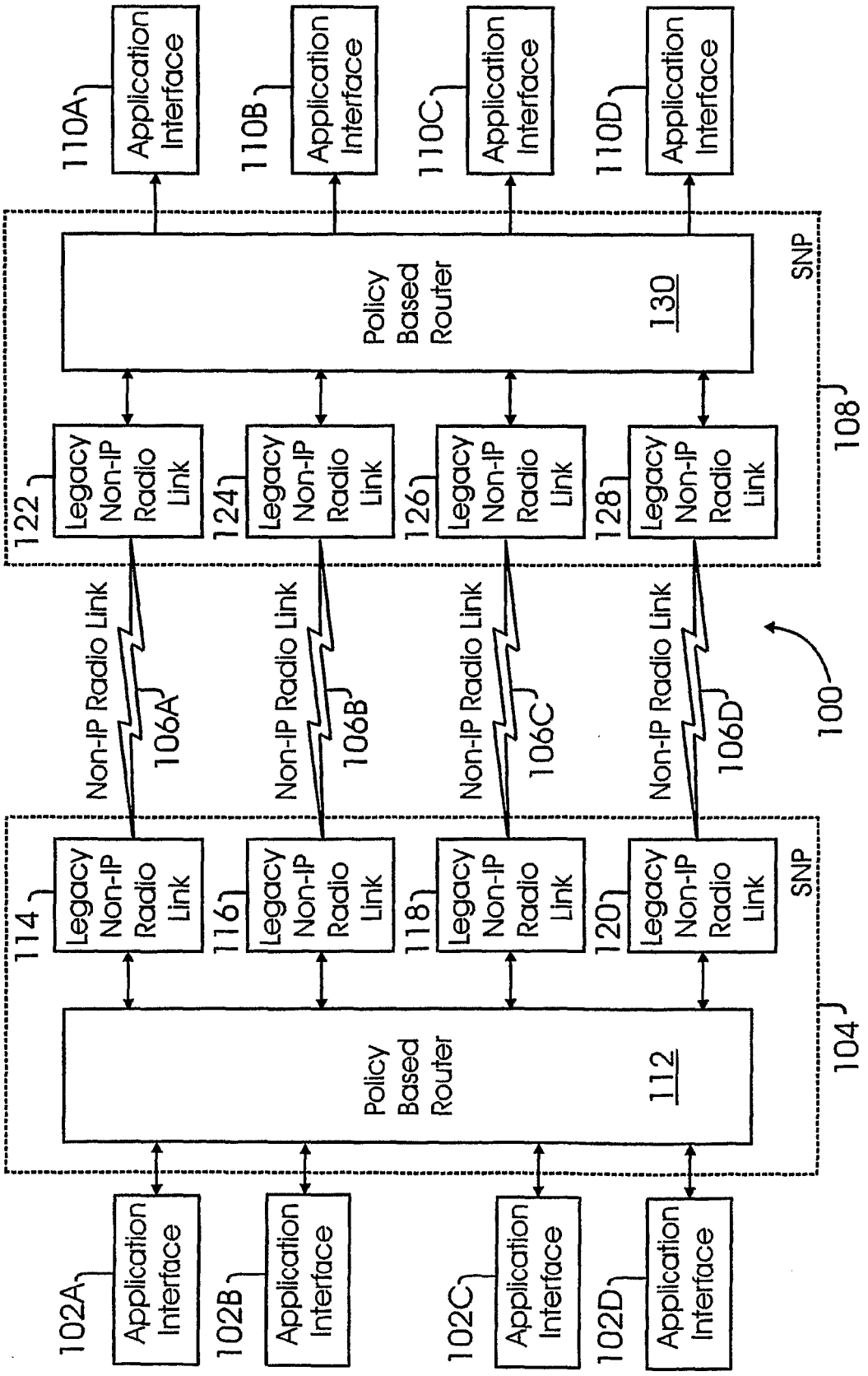

110A
Application Interface
110B
Application Interface
110C
Application Interface
110D
Application Interface
Policy Based Router
130
SNP
108
122
Legacy Non-IP Radio Link
124
Legacy Non-IP Radio Link
126
Legacy Non-IP Radio Link
128
Legacy Non-IP Radio Link
Non-IP Radio Link
106A
Non-IP Radio Link
106B
Non-IP Radio Link
106C
Non-IP Radio Link
106D
100
114
Legacy Non-IP Radio Link
116
Legacy Non-IP Radio Link
118
Legacy Non-IP Radio Link
120
Legacy Non-IP Radio Link
SNP
104
Policy Based Router
112
102A
Application Interface
102B
Application Interface
102C
Application Interface
102D
Application Interface

Figure 3

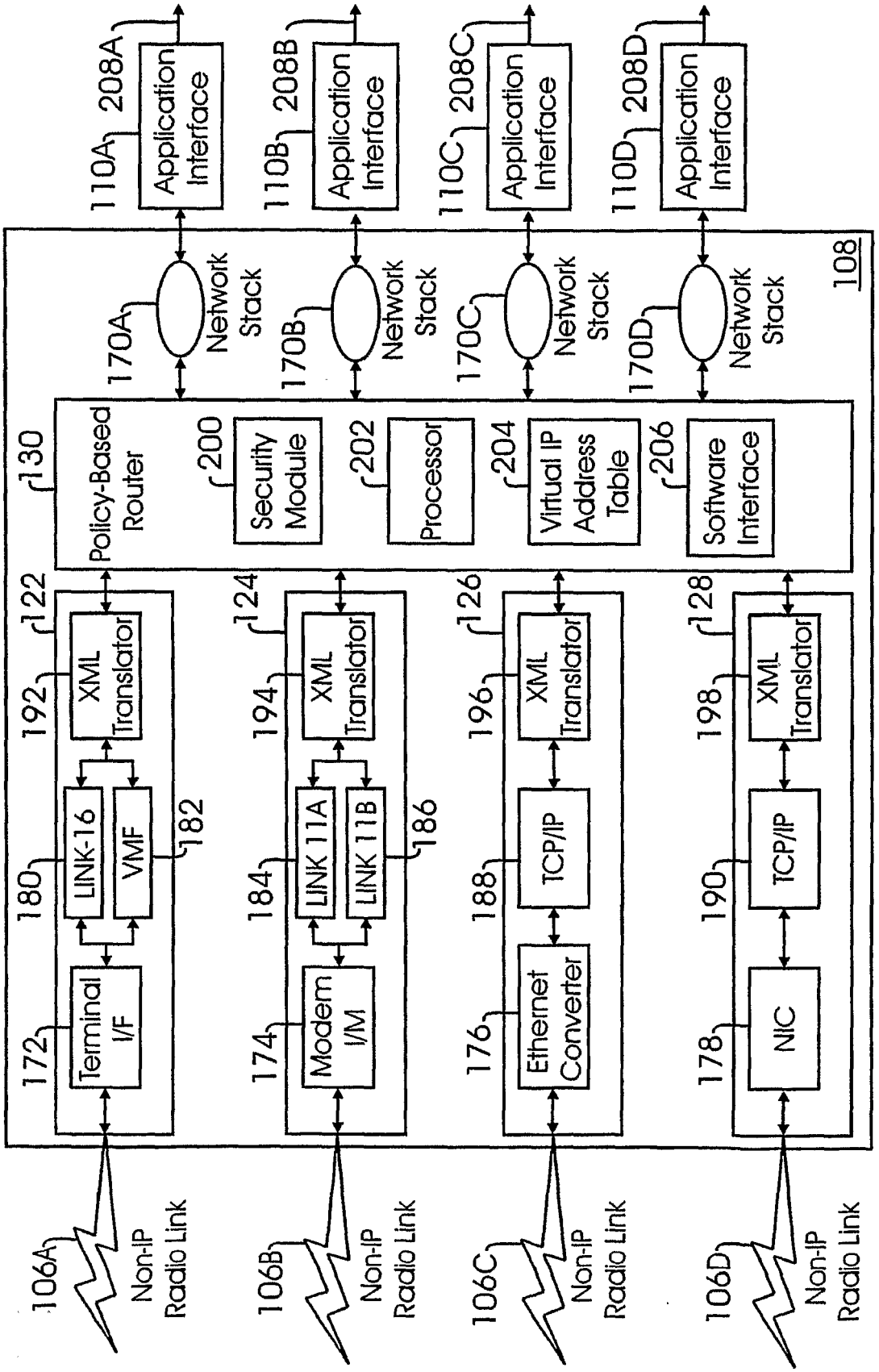

110A
208A
Application Interface
110B
208B
Application Interface
110C
208C
Application Interface
110D
208D
Application Interface
170A
Network Stack
170B
Network Stack
170C
Network Stack
170D
Network Stack
108
130
Policy-Based Router
200
Security Module
202
Processor
204
Virtual IP Address Table
206
Software Interface
122
192
XML Translator
180
LINK-16
VMF
182
172
Terminal I/F
124
194
XML Translator
184
LINK 11A
LINK 11B
186
174
Modem I/M
126
196
XML Translator
188
TCP/IP
176
Ethernet Converter
128
198
XML Translator
190
TCP/IP
178
NIC
106A
Non-IP Radio Link
106B
Non-IP Radio Link
106C
Non-IP Radio Link
106D
Non-IP Radio Link

Figure 4

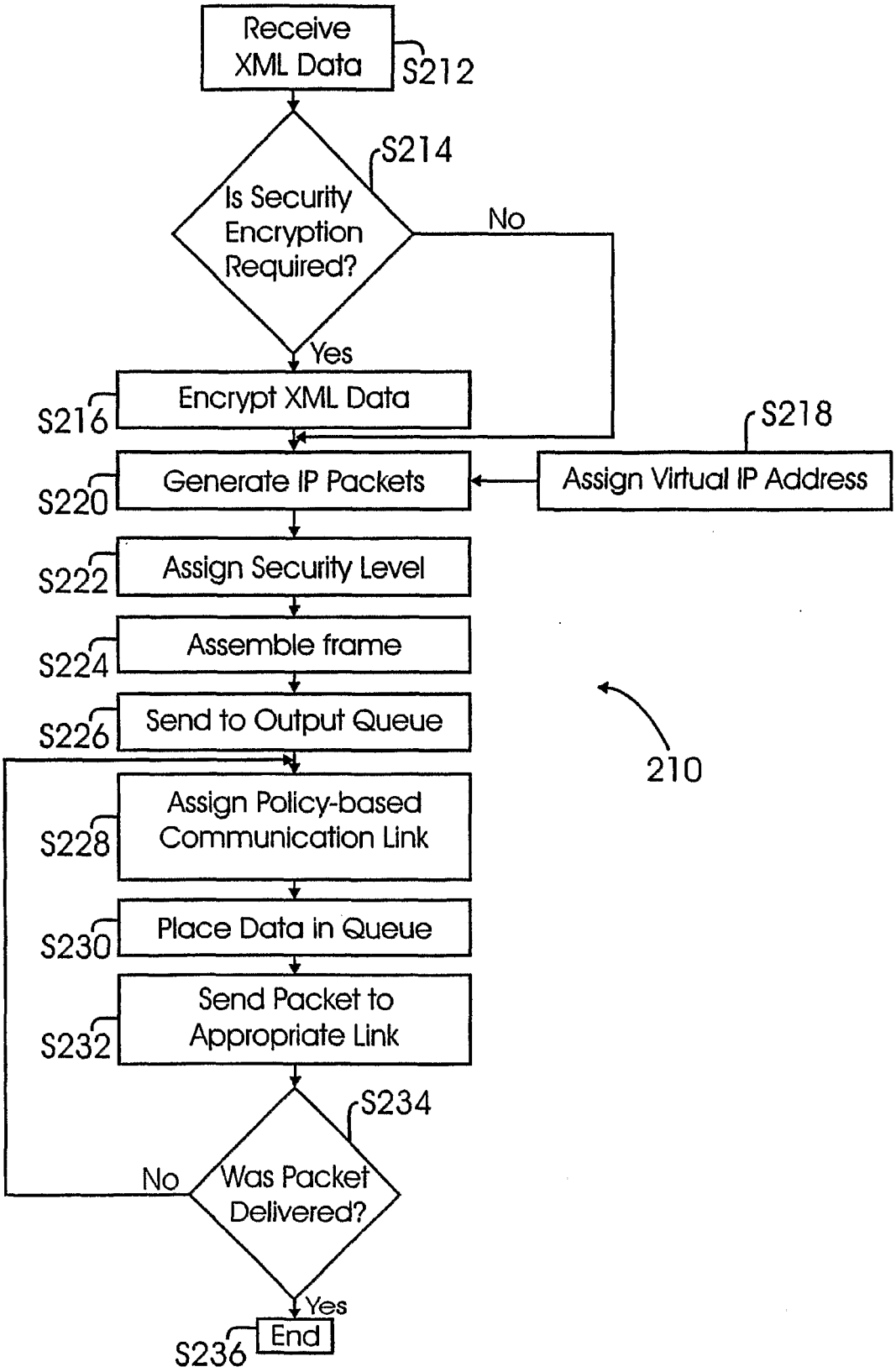

Receive XML Data
S212
S214
Is Security Encryption Required?
No
Yes
S216
Encrypt XML Data
S218
Assign Virtual IP Address
S220
Generate IP Packets
S222
Assign Security Level
S224
Assemble frame
S226
Send to Output Queue
210
S228
Assign Policy-based Communication Link
S230
Place Data in Queue
S232
Send Packet to Appropriate Link
S234
No
Was Packet Delivered?
Yes
S236
End

Figure 5

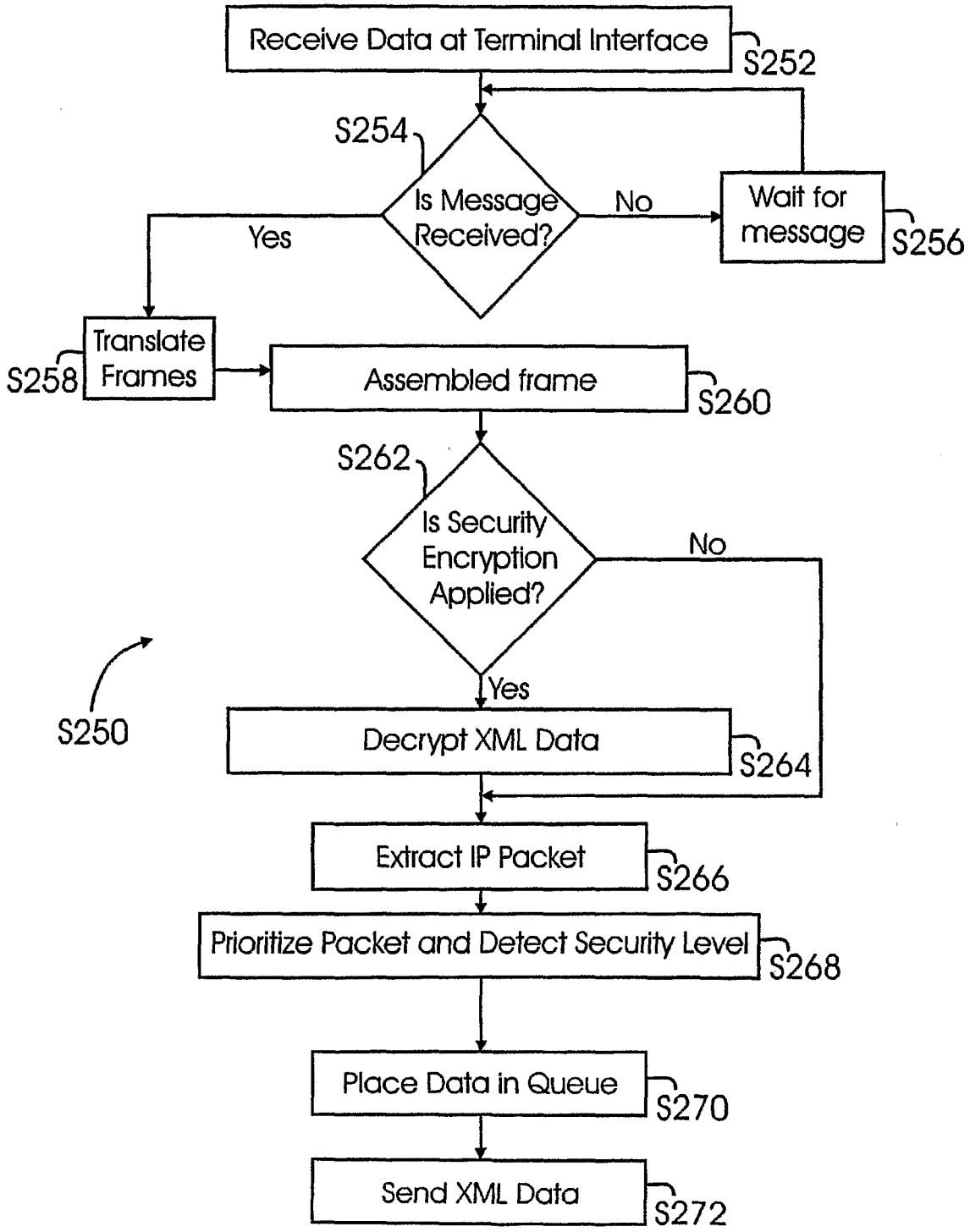

Receive Data at Terminal Interface
S252
S254
Is Message Received?
No
Wait for message
S256
Yes
Translate Frames
S258
Assembled frame
S260
S262
Is Security Encryption Applied?
No
Yes
S250
Decrypt XML Data
S264
Extract IP Packet
S266
Prioritize Packet and Detect Security Level
S268
Place Data in Queue
S270
Send XML Data
S272

Figure 6

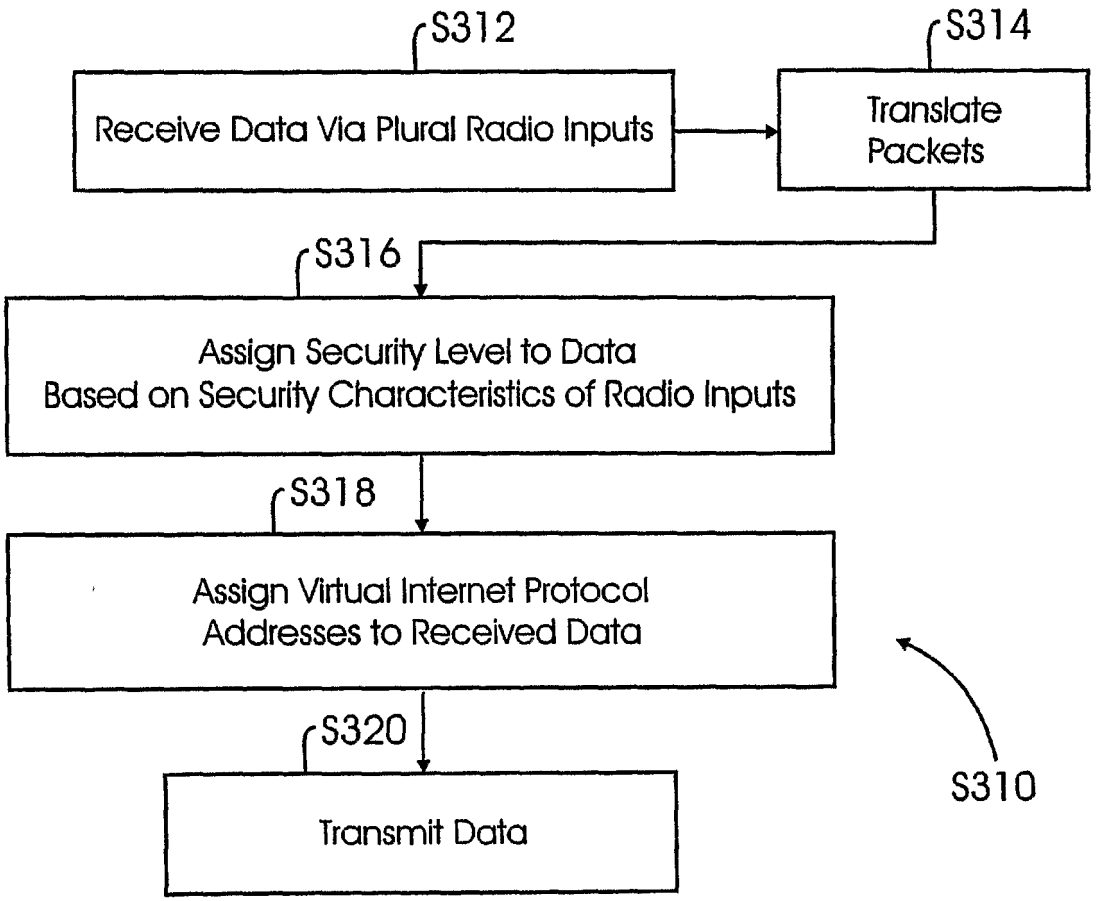

S312
Receive Data Via Plural Radio Inputs
S314
Translate Packets
S316
Assign Security Level to Data Based on Security Characteristics of Radio Inputs
S318
Assign Virtual Internet Protocol Addresses to Received Data
S320
Transmit Data
S310

Figure 7

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 03021866 A **[0009]**
- WO 0126338 A **[0012]**

Non-patent literature cited in the description

- Extensible Markup Language (''XML). W3C Consortium, October 2000 **[0037]**